REMARKS

Applicant notes that the examiner indicated that claims 8-17, 23-24 and 39-40, would be allowable if rewritten to include all of the limitations of the base claim and any intervening claims. Applicant thanks the examiner for the indication of allowable subject matter. Applicant contends that all of the claims are allowable over the art of record, as is discussed below.

The examiner rejected claims 7, 21-22 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,304,262 B1 Maloney et al.(hereinafter Maloney).

The examiner stated: "Regarding Claim 7, 21, Maloney discloses the building of graph and the classifying of the attack see Col 10, Ln 37-45 & Col 6, Ln 64-Col 7, Ln 6."

Applicant's claim 7 calls for a method for thwarting denial of service attacks on a data center, the method comprising: producing a histogram of received network traffic for at least one parameter of network packets and characterizing an attack based on comparison of historical histograms with the produced histogram data for one or more parameters. These features are neither described nor suggested by Maloney.

Maloney describes at Col. 10 line 37-45:

> **Data stored in a flat text file by operation of the discovery tool 12 is utilized by the KB summation tool of the knowledge base tool set 96 to create a statistical matrix of the data contained in packet and session logs. For example, the instance of a protocol may be used as the Y access and the source IP address may be used as the X access. After selection of the packet or session log has been made, the KB summation tool screens the appropriate log file and displays available access criteria to create a graph.**

At Col. 9, line 64 to Col. 7, line 6, Maloney describes:

> **Following parsing of the knowledge base 16 the analytical engine 20 responds to the data for preparation and converting into vector-based nodal diagrams. Typically the analytical engine 20 creates associations between a number of different charts to determine if such data charts correlate or differentiate. Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Based on this analysis, the information security analysis system enables the development of resources for management of a network.**

Maloney uses data to build a graph, that is, "a statistical matrix of the data contained in packet and session logs. For example, the instance of a protocol may be used as the Y access and the source IP address may be used as the X access." Maloney fails to describe or suggest however, producing a histogram, and in particular fails to suggest producing a histogram for received network traffic for at least one parameter of network packets. The teaching "the instance of a protocol may be used as the Y access and the source IP address may be used as the X access." does not describe a histogram.

Moreover, Maloney neither describes nor suggests characterizing an attack based on comparison of historical histograms with the produced histogram data for one or more parameters. The examiner relies on a teaching from Maloney, where Maloney describes that:

> **Typically the analytical engine 20 creates associations between a number of different charts to determine if such data charts correlate or differentiate. Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Based on this analysis, the information security analysis system enables the development of resources for management of a network.**

Nothing in this general discussion suggests characterizing an attack based on comparison of historical histograms with the produced histogram data for one or more parameters, as in claim 7.

The examiner stated: "Regarding Claim 22, Maloney discloses the vector-based correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks and reduce dropping legitimate traffic see Col 6, Ln 63-Col 7 Ln 11." This excerpt from Maloney is reproduced below:

> **Following parsing of the knowledge base 16 the analytical engine 20 responds to the data for preparation and converting into vector-based nodal diagrams. Typically the analytical engine 20 creates associations between a number of different charts to determine if such data charts correlate or differentiate. Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Based on this analysis, the information security analysis system enables the development of resources for management of a network.**
>
> **The analytical engine 20 analyzes network data to relate knowledge base data to session data, packet data, and alert data as these relationships are utilized to determine who has been talking to whom as well as the content of the traffic for specific protocols.**

Maloney, whether in the above passage or elsewhere neither discloses nor suggests a process to correlate suspicious parameters to reduce blocking of legitimate traffic. Rather, Maloney discloses a technique to correlate relationships among multiple data sets in order to develop resources for management of a network.

The examiner rejected claims 1-6, 18-20, 22, and 28-37 under 35 U.S.C. 103(a), as being unpatentable over U.S. Patent 6,301,668 B1 Gleichauf et al. (hereinafter Gleichauf) in view of U.S. Patent 6,304,262 B1 to Maloney et al.(hereinafter Maloney).

> **Regarding Claim 1, Gleichauf discloses a detection process to determine to if the parameter has exceeded normal values see Col 8 Ln 46- Col 9 Ln 3; the filtering process based on the characteristic and being incorporated in a firewall, router, and ID system see Col 1 Ln 22-31 & Col 4 Ln 33-39. Gleichauf does not disclose a process of building an graph to and to classify the attack. However, Maloney discloses the building of graph and the classifying of the attack see Col 10 Ln 37-45. It would be obvious to one having ordinary skll in the art at the time of the invention to include the building of graph and the classifying of the attack in the invention of Gleichauf in order to allow the systems administrator to take appropriate measures as taught in Maloney see Col 7 Ln 40-Col 8 Ln 12. And further, Gleichauf discloses the possibly of visual representation see Fig. 3 item 64, thus the inclusion of a building a graph would be reasonable successful.**

Applicant's claim 1 is distinct over Gleichauf taken separately or in combination with Maloney, since the combination of references fails to suggest: a process that monitors network traffic through a monitoring device disposed between a data center and a network for thwarting denial of service attacks on the data center *** a detection process to determine if the values of a parameter exceed normal values for the parameter to indicate an attack on the data center and a characterization process to build a histogram for the parameter to compute significant outliers in a parameter and classify the attack. The combination of references also fails to suggest a filtering process that provides filtering of network packets based on the characterization process.

Gleichauf is directed to a vulnerability assessment system. As such, Gleichauf fails to suggest a process that monitors network traffic through a monitoring device disposed between a data center and a network for thwarting denial of service attacks on the data center and a detection process to determine if the values of a parameter exceed normal values for the parameter to indicate an attack on the data center. The examiner contends that Gleichauf teaches

this at Col 8, Ln 46-Col 9, Ln 3 and the filtering process based on the characteristic at Col 1, Ln 22-31 & Col 4, Ln 33-39.

The teaching at Col. 8, line 46 to col. 9, line 3 deals with a vulnerability assessment process, not a process to thwart a denial of service attack. (See for example col. 7, lines 65-66.) Moreover, Gleichauf in col. 8 fails to teach "a detection process to determine if the values of a parameter for the network traffic exceed normal values for the parameter to indicate an attack on the data center." Rather, (in Col. 8 and Col. 9) Gleichauf discusses protocol analysis 111 and attack signatures 113. Gleichauf discloses that these processes 111 and 113 occur in protocol engine 24 and signature engine 26, at Col. 9, Line 55.

> **Further in operation, protocol engine 24 performs a plurality of protocol analyses upon monitored traffic on network backbone 14 in order to detect attacks upon the network. Attacks upon the network, as mentioned above, are defined herein to include unauthorized accesses, policy violations, and patterns of misuse. Protocol engine 24 can perform, for example, the following protocol analyses upon monitored traffic on network backbone 14: checksum verification (IP, TCP, UDP, ICMP, etc.), IP fragment reassembly, TCP stream reassembly, protocol verification (such as insuring the IP header length is correct and the TCP data gram is not truncated), and timeout calculations.**
>
> **Signature engine 26 is coupled to protocol engine 24 and can perform further analysis tasks in order to detect attacks upon network backbone 14. Signature engine 26 compares monitored traffic with attack signatures 30. Attack signatures 30 can comprise, for example, a rules-based hierarchy of traffic signatures of known policy violations. Signature engine 26 can compare packets from the network traffic with such attack signatures 30 such that policy violations can be discovered.**

Neither of these teachings suggests "a detection process to determine if the values of a parameter for the network traffic exceed normal values for the parameter to indicate an attack on the data center." A signature engine does not determine if values of a parameter exceed normal values for the parameter, but rather seeks to match a signature of an attack to known attack signatures." A protocol engine while performing protocol analysis again does not determine if values of a parameter exceed normal values for the parameter, but rather performs: "protocol analyses upon monitored traffic on network backbone 14: checksum verification (IP, TCP, UDP, ICMP, etc.), IP fragment reassembly, TCP stream reassembly, protocol verification (such as insuring the IP header length is correct and the TCP data gram is not truncated), and timeout calculations." [At Col. 9, Lines 50-54]

The examiner relies on Maloney to teach "a characterization process to build a histogram for the parameter to compute significant outliers in a parameter and classify the attack." As discussed above, Maloney at Col. 10, lines 37-45, describes using data to build a graph, however the example that Maloney describes relates to: "a statistical matrix of the data contained in packet and session logs. For example, the instance of a protocol may be used as the Y access and the source IP address may be used as the X access." Maloney fails to describe or suggest producing a histogram, and in particular for the parameter to compute significant outliers in a parameter and classify the attack.

Moreover, Applicant contends that the combination of Gleichauf and Maloney is not suggested. The examiner contends that:

> **It would be obvious to one having ordinary skll in the art at the time of the invention to include the building of graph and the classifying of the attack in the invention of Gleichauf in order to allow the systems administrator to take appropriate measures as taught in Maloney see Col 7 Ln 40-Col 8 Ln 12. And further, Gleichauf discloses the possibly of visual representation see Fig. 3 item 64, thus the inclusion of a building a graph would be reasonable successful.**

Gleichauf, as discussed earlier, deals with vulnerability assessment, whereas, Maloney deals with an information security analysis system. One would not be motivated by Gleichauf to look to an information security analysis system to add the features of the histogram, since in claim 1 the histogram is used to detect a denial of service attack and not merely used for "visual representation," as the examiner contends.

Applicant contends therefore that the combination of Gleichauf and Maloney fail to suggest claim 1. Applicant further contends that claims 2-6 add distinct limitations to claim 1 and that claims 18-20, which depend from claim 7 are allowable at least for the reasons discussed in claim 7. In addition, claim 22 is allowable with claim 21 and claims 28-37 are allowable for analogous reasons discussed in claim 7.

The examiner rejected Claim 25 under 35 U.S.C. 103(a) as being unpatentable over U.S. Maloney in view of Gleichauf.

The examiner stated:

Regarding Claim 25, Maloney does not discloses the installing filters on routers, having data collectors, and parameters. However, Gleichauf discloses the installing of filters on routers see Col 4 Ln 33-39. Gleichauf discloses the data collector see Fig. 2 item 36. And further, Gleichauf discloses the parameters including a source IP protocol, IP length, TCPIUDP ports see Col 6 Ln 24-35. It would be obvious to one having ordinary skill in the art at the time of the invention to include installing filters on routers in the invention of Maloney in order to increase security as taught in Gleichauf see Col 4 Ln 33-39.

Claim 25 is allowable, since the references fail to suggest the features of the base claim 21, and fail to suggest that the device is a gateway device that is adaptable to dynamically install filters on nearby routers.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Applicant has enclosed an Information Disclosure Statement that sets forth references from other cases of the assignee of this application.

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 10/12/04

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906